

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets

(11) Veröffentlichungsnummer:

(11) Publication number:

(11) Numéro de publication:

EP 1 166 494 A0

Internationale Anmeldung veröffentlicht durch die
Weltorganisation für geistiges Eigentum unter der Nummer:

WO 00/59156 (art. 158 des EPÜ).

International application published by the World
Intellectual Property Organisation under number:

WO 00/59156 (art. 158 of the EPC).

Demande internationale publiée par l'Organisation
Mondiale de la Propriété sous le numéro:

WO 00/59156 (art. 158 de la CBE).



DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁷ : H04L 9/30, G06F 7/72	A1	(11) Numéro de publication internationale: WO 00/59156 (43) Date de publication internationale: 5 octobre 2000 (05.10.00)
---	----	--

(21) Numéro de la demande internationale: PCT/FR00/00603

(22) Date de dépôt international: 13 mars 2000 (13.03.00)

(30) Données relatives à la priorité:
99/03921 26 mars 1999 (26.03.99) FR

(71) Déposant (pour tous les Etats désignés sauf US): GEMPLUS [FR/FR]; Nonnenmacher, Bernard, Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F-13881 Gémenos (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (US seulement): CORON, Jean-Sébastien [FR/FR]; 4 rue Léon de Lagrange, F-75015 Paris (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus, Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F-13881 Gémenos (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

Avec rapport de recherche internationale.

(54) Title: COUNTERMEASURE PROCEDURES IN AN ELECTRONIC COMPONENT IMPLEMENTING AN ELLIPTICAL CURVE TYPE PUBLIC KEY ENCRYPTION ALGORITHM

(54) Titre: PROCEDES DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE DE TYPE COURBE ELLIPTIQUE

(57) Abstract

Elliptical curve based cryptographic algorithms are public key algorithms offering a shorter calculation time and smaller key sizes in comparison with RSA. The application thereof in a chipcard type environment has proved to be vulnerable to differential power analysis (DPA) attacks. The invention describes a countermeasure procedure enabling positive action to be taken against DPA type attacks. The countermeasure does not reduce performance and is easy to use in a chipcard type component.

(57) Abrégé

Les algorithmes cryptographiques à base de courbes elliptiques sont des algorithmes à clef publique présentant sur RSA l'avantage de temps de calcul présentant sur RSA l'avantage de temps de calcul plus faible et de taille de clefs plus petites. Il est apparu que leur application dans le cadre d'un environnement de type carte à puce était vulnérable à des attaques de type DPA (Differential Power Analysis). La présente invention consiste en la description d'un procédé de contre-mesure permettant de se prémunir contre ce type d'attaque DPA. Cette contre-mesure ne diminue pas les performances et est facilement utilisable dans un composant de type carte à puce.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakhstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

PROCEDES DE CONTRE-MESURE DANS UN COMPOSANT
ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE
CRYPTOGRAPHIE A CLE PUBLIQUE DE TYPE COURBE ELLIPTIQUE

La présente invention concerne un procédé de
contre-mesure dans un composant électronique
mettant en œuvre un algorithme de chiffrement à
5 clé publique de type courbe elliptique.

Dans le modèle classique de la cryptographie à
clef secrète, deux personnes désirant
communiquer par l'intermédiaire d'un canal non
10 sécurisé doivent au préalable se mettre d'accord
sur une clé secrète de chiffrement K. La
fonction de chiffrement et la fonction de
déchiffrement utilisent la même clef K.
L'inconvénient du système de chiffrement à clé
15 secrète est que ledit système requiert la
communication préalable de la clé K entre les
deux personnes par l'intermédiaire d'un canal
sécurisé, avant qu'un quelconque message chiffré
ne soit envoyé à travers le canal non sécurisé.
20 Dans la pratique, il est généralement difficile
de trouver un canal de communication
parfaitement sécurisé, surtout si la distance
séparant les deux personnes est importante. On
entend par canal sécurisé un canal pour lequel
25 il est impossible de connaître ou de modifier
les informations qui transitent par ledit canal.
Un tel canal sécurisé peut être réalisé par un
câble reliant deux terminaux, possédés par les
deux dites personnes.

Le concept de cryptographie à clef publique fut inventé par Whitfield DIFFIE et Martin HELLMAN en 1976. La cryptographie à clef publique permet de résoudre le problème de la distribution des
5 clefs à travers un canal non sécurisé. Le principe de la cryptographie à clef publique consiste à utiliser une paire de clefs, une clef publique de chiffrement et une clef privée de déchiffrement. Il doit être calculatoirement
10 infaisable de trouver la clef privée de déchiffrement à partir de la clef publique de chiffrement. Une personne A désirant communiquer une information à une personne B utilise la clef publique de chiffrement de la personne B. Seule
15 la personne B possède la clef privée associée à sa clef publique. Seule la personne B est donc capable de déchiffrer le message qui lui est adressé.

20 Un autre avantage de la cryptographie à clé publique sur la cryptographie à clé secrète est que la cryptographie à clef publique permet l'authentification par l'utilisation de signature électronique.

25

La première réalisation de schéma de chiffrement à clef publique fut mis au point en 1977 par Rivest, Shamir et Adleman, qui ont inventé le système de chiffrement RSA. La sécurité de RSA
30 repose sur la difficulté de factoriser un grand nombre qui est le produit de deux nombres premiers.

Depuis, de nombreux systèmes de chiffrement à clef publique ont été proposés, dont la sécurité repose sur différents problèmes calculatoires : (cette liste n'est pas exhaustive).

5

- Sac à dos de Merckle-Hellman :

Ce système de chiffrement est basé sur la difficulté du problème de la somme de sous-ensembles.

10

- McEliece :

Ce système de chiffrement est basé sur la théorie des codes algébriques. Il est basé sur le problème du décodage de codes linéaires.

15

- ElGamal :

Ce système de chiffrement est basé sur la difficulté du logarithme discret dans un corps fini.

20

- Courbes elliptiques :

Le système de chiffrement à courbe elliptique constitue une modification de systèmes cryptographiques existant pour les appliquer au domaine des courbes elliptiques.

25

L'utilisation de courbes elliptiques dans des systèmes cryptographiques fut proposé indépendamment par Victor Miller et Neal Koblitz en 1985. Les applications réelles des courbes elliptiques ont été envisagées au début des années 1990.

30

L'avantage de cryptosystèmes à base de courbe elliptique est qu'ils fournissent une sécurité équivalente aux autres cryptosystèmes mais avec des tailles de clef moindres. Ce gain en taille
5 de clé implique une diminution des besoins en mémoire et une réduction des temps de calcul, ce qui rend l'utilisation des courbes elliptiques particulièrement adaptées pour des applications de type carte à puce.

10

Une courbe elliptique sur un corps fini $GF(q^n)$ (q étant un nombre premier et n un entier) est l'ensemble des points (x,y) avec x l'abscisse et y l'ordonnée appartenant à $GF(q^n)$
15 solution de l'équation :

$$y^2 = x^3 + ax + b$$

si q est supérieur ou égal à 3

$$\text{et } y^2 + x*y = x^3 + a*x^2 + b$$

si $q=2$.

20

Il existe 2 procédés pour représenter un point d'une courbe elliptique :

Premièrement, la représentation en coordonnées affine; dans ce procédé, un point P de la courbe elliptique est représenté par ses
25 coordonnées (x,y) .

Deuxièmement, la représentation en coordonnées projectives.

L'avantage de la représentation en coordonnées
30 projectives est qu'elle permet d'éviter les divisions dans le corps fini, lesdites divisions étant les opérations les plus coûteuses en temps de calcul.

La représentation en coordonnées projectives le plus couramment utilisée est celle consistant à représenter un point P de la courbe elliptique par les coordonnées (X, Y, Z) , telles que $x = X/Z$ et
5 $y = Y/Z^3$.

Les coordonnées projectives d'un point ne sont pas uniques parce que le triplet (X, Y, Z) et le triplet $(\lambda^2 X, \lambda^3 Y, \lambda Z)$ représentent le même point quelque soit l'élément λ appartenant au
10 corps fini sur lequel est défini la courbe elliptique.

Les 2 classes de courbes les plus utilisées en cryptographie sont les suivantes :

15

1) Courbes définies sur le corps fini $GF(p)$ (ensemble des entiers modulo p , p étant un nombre premier) ayant pour équation
 $y^2 = x^3 + a \cdot x + b$

20

2) Courbes définies sur le corps fini $GF(2^n)$ ayant pour équation
 $y^2 + x \cdot y = x^3 + a \cdot x^2 + b$

25 Pour chacune de ces deux classes de courbes, on définit les opérations d'addition de point et de doublement de point.

L'addition de point est l'opération qui étant donné deux points P et Q calcule la somme $R = P + Q$,
30 R étant un point de la courbe dont les coordonnées s'expriment à l'aide des coordonnées des points P et Q suivant des formules dont l'expression est donnée dans l'ouvrage

" Elliptic curve public key cryptosystem " par Alfred J. Menezes.

Le doublement de point est l'opération qui, étant donné un point P , calcule le point $R=2 \cdot P$,
5 R étant un point de la courbe dont les coordonnées s'expriment à l'aide des coordonnées du point P suivant des formules dont l'expression est donnée dans l'ouvrage
" Elliptic curve public key cryptosystem " par
10 Alfred J. Menezes.

Les opérations d'addition de point et de doublement de point permettent de définir une
15 opération de multiplication scalaire : étant donné un point P appartenant à une courbe elliptique et un entier d , le résultat de la multiplication scalaire de P par d est le point Q tel que $Q=d \cdot P=P+P+\dots+P$ d fois.

20

La sécurité des algorithmes de cryptographie sur courbes elliptiques est basée sur la difficulté du problème du logarithme discret sur courbes elliptiques, ledit problème consistant à partir
25 de deux points Q et P appartenant à une courbe elliptique E , de trouver, s'il existe, un entier x tel que $Q=x \cdot P$

Il existe de nombreux algorithmes
30 cryptographiques basés sur le problème du logarithme discret. Ces algorithmes sont facilement transposables aux courbes elliptiques.

Ainsi, il est possible de mettre en œuvre des algorithmes assurant l'authentification, la confidentialité, le contrôle d'intégrité et l'échange de clé.

5

Un point commun à la plupart des algorithmes cryptographiques basés sur les courbes elliptiques est qu'ils comprennent comme paramètre une courbe elliptique définie sur un corps fini et un point P appartenant à cette courbe elliptique. La clé privée est un entier d choisi aléatoirement. La clef publique est un point de la courbe Q tel que $Q=d \cdot P$. Ces algorithmes cryptographiques font généralement intervenir une multiplication scalaire dans le calcul d'un point $R=d \cdot T$ où d est la clef secrète.

Dans le paragraphe ci dessous, on décrit un algorithme de chiffrement à base de courbe elliptique. Ce schéma est analogue au schéma de chiffrement d'El Gamal. Un message m est chiffré de la manière suivante :

25 Le chiffreur choisit un entier k aléatoirement et calcule les points $k \cdot P=(x_1, y_1)$ et $k \cdot Q=(x_2, y_2)$ de la courbe, et l'entier $c= x_2 + m$. Le chiffré de m est le triplet (x_1, y_1, c) .

Le déchiffreur qui possède d déchiffre m en calculant :

$$(x'_2, y'_2)=d(x_1, y_1) \text{ et } m=c-x'_2$$

Pour réaliser les multiplications scalaires nécessaires dans les procédés de calcul décrits précédemment, plusieurs algorithmes existent :

- 5 - Algorithme " double and add " ;
- Algorithme " addition-soustraction "
- Algorithme avec chaines d'addition ;
- Algorithme avec fenêtre ;
- Algorithme avec représentation signée.

10

Cette liste n'est pas exhaustive. L'algorithme le plus simple et le plus utilisé est l'algorithme " double and add ". L'algorithme " double and add " prend en entrée un point P appartenant à une courbe elliptique donnée et un entier d. L'entier d est noté $d=(d(t), d(t-1), \dots, d(0))$, où $(d(t), d(t-1), \dots, d(0))$ est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible.

15

20 L'algorithme retourne en sortie le point $Q=d.P$.

L'algorithme " double and add " comporte les 3 étapes suivantes :

- 25 1) Initialiser le point Q avec la valeur P
- 2) Pour i allant de t-1 à 0 exécuter :
 - 2a) Remplacer Q par 2Q
 - 2b) Si $d(i)=1$ remplacer Q par $Q+P$
- 3) Retourner Q.

30

Il est apparu que l'implémentation sur carte à puce d'un algorithme de chiffrement à clé publique du type courbe elliptique était vulnérable à des attaques consistant en une analyse différentielle de consommation de courant permettant de retrouver la clé privée de déchiffrement. Ces attaques sont appelées attaques DPA, acronyme pour Differential Power Analysis. Le principe de ces attaques DPA repose sur le fait que la consommation de courant du microprocesseur exécutant des instructions varie selon la donnée manipulée.

En particulier, lorsqu'une instruction manipule une donnée dont un bit particulier est constant, la valeur des autres bits pouvant varier, l'analyse de la consommation de courant liée à l'instruction montre que la consommation moyenne de l'instruction n'est pas la même suivant que le bit particulier prend la valeur 0 ou 1. L'attaque de type DPA permet donc d'obtenir des informations supplémentaires sur les données intermédiaires manipulées par le microprocesseur de la carte lors de l'exécution d'un algorithme cryptographique. Ces informations supplémentaires peuvent dans certain cas permettre de révéler les paramètres privés de l'algorithme de déchiffrement, rendant le système cryptographique non sûr.

Dans la suite de ce document on décrit un procédé d'attaque DPA sur un algorithme de type courbe elliptique réalisant une opération du type multiplication scalaire d'un point P par un entier d , l'entier d étant la clé secrète. Cette
5 attaque permet de révéler directement la clé secrète d . Elle compromet donc gravement la sécurité de l'implémentation de courbes elliptiques sur une carte à puce.

10

La première étape de l'attaque est l'enregistrement de la consommation de courant correspondant à l'exécution de l'algorithme "double and add" décrit précédemment pour N
15 points distincts $P(1), \dots, P(N)$. Dans un algorithme à base de courbes elliptiques, le microprocesseur de la carte à puce va effectuer N multiplications scalaires $d.P(1), \dots, d.P(N)$.

20 Pour la clarté de la description de l'attaque, on commence par décrire une méthode permettant d'obtenir la valeur du bit $d(t-1)$ de la clé secrète d , où $(d(t), d(t-1), \dots, d(0))$ est la représentation binaire de d , avec $d(t)$ le bit de
25 poids fort et $d(0)$ le bit de poids faible. On donne ensuite la description d'un algorithme qui permet de retrouver la valeur de d .

On groupe les points $P(1)$ à $P(N)$ suivant la
30 valeur du dernier bit de l'abscisse de $4.P$, où P désigne un des points $P(1)$ à $P(N)$. Le premier groupe est constitué des points P tels que le dernier bit de l'abscisse de $4.P$ est égal à 1.

Le second groupe est constitué des points P tels que le dernier bit de l'abscisse de $4.P$ est égal à 0. On calcule la moyenne des consommations de courant correspondant à chacun des deux groupes, et on calcule la courbe de différence entre ces deux moyennes.

Si le bit $d(t-1)$ de d est égal à 0, alors l'algorithme de multiplication scalaire précédemment décrit calcule et met en mémoire la valeur de $4.P$. Cela signifie que lors de l'exécution de l'algorithme dans une carte à puce, le microprocesseur de la carte va effectivement calculer $4.P$. Dans ce cas, dans le premier groupe de message le dernier bit de la donnée manipulée par le microprocesseur est toujours à 1, et dans le deuxième groupe de message le dernier bit de la donnée manipulée est toujours à 0. La moyenne des consommations de courant correspondant à chaque groupe est donc différente. Il apparaît donc dans la courbe de différence entre les 2 moyennes un pic de différentiel de consommation de courant.

Si au contraire le bit $d(t-1)$ de d est égal à 1, l'algorithme d'exponentiation décrit précédemment ne calcule pas le point $4.P$. Lors de l'exécution de l'algorithme par la carte à puce, le microprocesseur ne manipule donc jamais la donnée $4.P$. Il n'apparaît donc pas de pic de différentiel de consommation.

Cette méthode permet donc de déterminer la valeur du bit $d(t-1)$ de d .

L'algorithme décrit dans le paragraphe suivant
5 est une généralisation de l'algorithme précédant. Il permet de déterminer la valeur de la clé secrète d .

On définit l'entrée par N points notés $P(1)$ à
10 $P(N)$ correspondant à N calculs réalisés par la carte à puce et la sortie par un entier h .

Ledit algorithme s'effectue de la manière suivante en trois étapes.

15

1) Exécuter $h=1$;

2) Pour i allant de $t-1$ à 1, exécuter :

2)1) Classer les points $P(1)$ à $P(N)$ suivant la valeur du dernier bit de l'abscisse de $(4 \cdot h) \cdot P$;

20 2)2) Calculer la moyenne de consommation de courant pour chacun des deux groupes ;

2)3) Calculer la différence entre les 2 moyennes ;

25 2)4) Si la différence fait apparaître un pic de différentiel de consommation, faire $h=h \cdot 2$;
sinon faire $h=h \cdot 2 + 1$;

3) Retourner h .

L'algorithme précédent fournit un entier h tel
30 que $d=2 \cdot h$ ou $d=2 \cdot h + 1$. Pour obtenir la valeur de d , il suffit ensuite de tester les deux hypothèses possibles.

L'attaque de type DPA décrite permet donc de retrouver la clé privée d.

Le procédé de l'invention consiste en
5 l'élaboration d'une contre mesure permettant de se prémunir contre l'attaque DPA décrite précédemment. Cette contre mesure utilise la représentation des points de la courbe elliptique en coordonnées projectives.

10

Comme il a été expliqué précédemment, le représentant d'un point en coordonnées projectives n'est pas unique. Si le corps fini sur lequel est défini la courbe elliptique
15 comprend n éléments, il est possible de choisir un représentant parmi $n-1$ possibles.

En choisissant un représentant aléatoire d'un point sur lequel on effectue un calcul, les valeurs intermédiaires du calcul deviennent
20 elles-mêmes aléatoires et donc imprévisibles de l'extérieur, ce qui rend l'attaque DPA précédemment décrite impossible.

Le procédé de la contre mesure consiste en une
25 modification des opérations d'addition de point et de doublement de point de courbe elliptiques définies sur les corps finis $GF(p)$ pour p premier et $GF(2^n)$. La modification des opérations d'addition de point et de doublement
30 de point de courbes elliptiques définies sur les corps finis $GF(p)$ pour p premier et $GF(2^n)$ s'applique quelque soit l'algorithme utilisé pour réaliser ces opérations.

Le procédé de la contre mesure consiste également en la définition de 4 variantes dans l'opération de multiplication scalaire. Ces 4 variantes s'appliquent quelque soit l'algorithme
5 utilisé pour réaliser l'opération de multiplication scalaire.

Dans ce paragraphe, on décrit la modification de l'algorithme de doublement de point d'une courbe
10 elliptique définie sur le corps fini $GF(p)$, où p est un nombre premier. La courbe elliptique est donc définie par l'équation suivante :

$$y^2 = x^3 + a \cdot x + b$$

15

où a et b sont des paramètres entiers fixés au départ.

Les coordonnées projectives du point
20 $Q = (X2, Y2, Z2)$ tel que $Q = 2 \cdot P$ avec $P = (X1, Y1, Z1)$ sont calculées par le procédé suivant en 6 étapes. Dans chacune des étapes, les calculs sont effectués modulo p .

- 25 1) Calculer $M = 3 \cdot X1^2 + a \cdot Z1^4$;
2) Calculer $Z2 = 2 \cdot Y1 \cdot Z1$;
3) Calculer $S = 4 \cdot X1 \cdot Y1^2$;
4) Calculer $X2 = M^2 - 2 \cdot S$;
5) Calculer $T = 8 \cdot Y1^4$;
30 6) Calculer $Y2 = M \cdot (S - X2) - T$.

Le procédé de la contre mesure consiste en une modification du procédé précédent.

Le nouveau procédé de doublement de point d'une courbe elliptique définie sur le corps fini $GF(p)$ consiste en les 8 étapes suivantes :

- 5 1) Tirer au hasard un entier λ tel que $0 < \lambda < p$;
- 2) Calculer $X'1 = \lambda^2 * X1$, $Y'1 = \lambda^3 * Y1$ et $Z'1 = \lambda * Z1$;
- 3) Calculer $M = 3 * X'1^2 + a * Z'1^4$;
- 4) Calculer $Z2 = 2 * Y'1 * Z'1$;
- 5) Calculer $S = 4 * X'1 * Y'1^2$;
- 10 6) Calculer $X2 = M^2 - 2 * S$;
- 7) Calculer $T = 8 * Y'1^4$;
- 8) Calculer $Y2 = M * (S - X2) - T$.

Plus généralement, le procédé de la contre
15 mesure s'applique quelque soit le procédé (noté par la suite A) utilisé pour réaliser l'opération de doublement de point. Le procédé A est remplacé par le procédé A' en 3 étapes :

20 Entrée : un point $P = (X1, Y1, Z1)$ représenté en coordonnées projectives.

Sortie : une point $Q = (X2, Y2, Z2)$ représenté en coordonnés projectives tel que $Q = 2.P$

- 25 1) Tirer au hasard un entier λ tel que $0 < \lambda < p$;
- 2) Calculer $X'1 = \lambda^2 * X1$, $Y'1 = \lambda^3 * Y1$ et $Z'1 = \lambda * Z1$,
 $X'1$, $Y'1$ et $Z'1$ définissant les coordonnées
du point $P' = (X'1, Y'1, Z'1)$;
- 3) Calculer $Q = 2 * P'$ à l'aide de l'algorithme A.

Les variables manipulées au cours de l'exécution du procédé A' étant aléatoire, l'attaque DPA précédemment décrite ne s'applique plus.

5 Dans ce paragraphe, on décrit la modification de l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini $GF(p)$, où p est un nombre premier.

10 Les coordonnées projectives du point $R=(X_2, Y_2, Z_2)$ tel que $R=P+Q$ avec $P=(X_0, Y_0, Z_0)$ et $Q=(X_1, Y_1, Z_1)$ sont calculées par le procédé suivant en 12 étapes. Dans chacune des étapes, les calculs sont effectués modulo p .

15

1) Calculer $U_0=X_0*Z_1^2$;

2) Calculer $S_0=Y_0*Z_1^3$;

3) Calculer $U_1=X_1*Z_0^2$;

4) Calculer $S_1=Y_1*Z_0^3$;

20 5) Calculer $W=U_0-U_1$;

6) Calculer $R=S_0-S_1$;

7) Calculer $T=U_0+U_1$;

8) Calculer $M=S_0+S_1$;

9) Calculer $Z_2=Z_0*Z_1*W$;

25 10) Calculer $X_2=R^2-T*W^2$;

11) Calculer $V=T*W^2-2*X_2$;

12) Calculer $2*Y_2=V*R-M*W^3$.

30 Le procédé de la contre mesure consiste en une modification du procédé précédent. Le nouveau procédé d'addition de point d'une courbe elliptique définie sur le corps fini $GF(p)$ consiste en les 16 étapes suivantes :

- 1) Tirer au hasard un entier λ tel que $0 < \lambda < p$;
- 2) Remplacer X_0 par $\lambda^2 \cdot X_0$, Y_0 par $\lambda^3 \cdot Y_0$ et Z_0 par $\lambda \cdot Z_0$;
- 5 3) Tirer au hasard un entier μ tel que $0 < \mu < p$;
- 4) Remplacer X_1 par $\mu^2 \cdot X_1$, Y_1 par $\mu^3 \cdot Y_1$ et Z_1 par $\mu \cdot Z_1$;
- 5) Calculer $U_0 = X_0 \cdot Z_1^2$;
- 6) Calculer $S_0 = Y_0 \cdot Z_1^3$;
- 10 7) Calculer $U_1 = X_1 \cdot Z_0^2$;
- 8) Calculer $S_1 = Y_1 \cdot Z_0^3$;
- 9) Calculer $W = U_0 - U_1$;
- 10) Calculer $R = S_0 - S_1$;
- 11) Calculer $T = U_0 + U_1$;
- 15 12) Calculer $M = S_0 + S_1$;
- 13) Calculer $Z_2 = Z_0 \cdot Z_1 \cdot W$;
- 14) Calculer $X_2 = R^2 - T \cdot W^2$;
- 15) Calculer $V = T \cdot W^2 - 2 \cdot X_2$;
- 16) Calculer $2 \cdot Y_2 = V \cdot R - M \cdot W^3$.

20

Plus généralement, le procédé de la contre mesure s'applique quelque soit le procédé (noté par la suite A) utilisé pour réaliser l'opération d'addition de point. Le procédé A

25 est remplacé par le procédé A' en 5 étapes :

Entrée : deux points $P = (X_0, Y_0, Z_0)$ et $Q = (X_1, Y_1, Z_1)$ représentés en coordonnées projectives.

30 Sortie : le point $R = (X_2, Y_2, Z_2)$ représenté en coordonnées projectives tel que $R = P + Q$

- 1) Tirer au hasard un entier λ tel que $0 < \lambda < p$;
- 2) Remplacer X_0 par $\lambda^2 \cdot X_0$, Y_0 par $\lambda^3 \cdot Y_0$ et Z_0 par $\lambda \cdot Z_0$;
- 3) Tirer au hasard un entier μ tel que $0 < \mu < p$;
- 5 4) Remplacer X_1 par $\mu^2 \cdot X_1$, Y_1 par $\mu^3 \cdot Y_1$ et Z_1 par $\mu \cdot Z_1$;
- 5) Calcul de $R=P+Q$ à l'aide de l'algorithme A.

10 Les variables manipulées au cours de l'exécution du procédé A' étant aléatoire, l'attaque DPA précédemment décrite ne s'applique plus.

Dans ce paragraphe, on décrit la modification de l'algorithme de doublement de point d'une courbe elliptique définie sur le corps fini $GF(2^n)$. La

15 courbe elliptique est donc définie par l'équation suivante :

$$y^2 + x \cdot y = x^3 + a \cdot x^2 + b$$

20 où a et b sont des paramètres appartenant au corps fini $GF(2^n)$ fixés au départ. On définit c par l'équation:

$$c = b^{(2^{(n-2)})}.$$

25 Les coordonnées projectives du point $Q=(X_2, Y_2, Z_2)$ tel que $Q=2 \cdot P$ avec $P=(X_1, Y_1, Z_1)$ sont calculées par le procédé suivant en 4 étapes. Dans chacune des étapes, les calculs sont effectués dans le corps fini $GF(2^n)$.

- 1) Calculer $Z2 = X1 * Z1^2$;
- 2) Calculer $X2 = (X1 + c * Z1^2)^4$;
- 3) Calculer $U = Z2 + X1^2 + Y1 * Z1$;
- 4) Calculer $Y2 = X1^4 * Z2 + U * X2$.

5

Le procédé de la contre mesure consiste en une modification du procédé précédent. Le nouveau procédé de doublement de point d'une courbe elliptique définie sur le corps fini $GF(2^n)$

10 consiste en les 6 étapes suivantes :

- 1) Tirer au hasard un élément non nul λ de $GF(2^n)$;
- 2) Calculer $X'1 = \lambda^2 * X1$, $Y'1 = \lambda^3 * Y1$, $Z'1 = \lambda * Z1$;
- 15 3) Calculer $Z2 = X'1 * Z'1^2$;
- 4) Calculer $X2 = (X'1 + c * Z'1^2)^4$;
- 5) Calculer $U = Z2 + X'1^2 + Y'1 * Z'1$;
- 6) Calculer $Y2 = X'1^4 * Z2 + U * X2$.

20 Plus généralement, le procédé de la contre mesure s'applique quelque soit le procédé (noté par la suite A) utilisé pour réaliser l'opération de doublement de point. Le procédé A est remplacé par le procédé A' en 3 étapes :

25

Entrée : un point $P = (X1, Y1, Z1)$ représenté en coordonnées projectives.

Sortie : un point $Q = (X2, Y2, Z2)$ représenté en coordonnées projectives tel que $Q = 2.P$

30

1) Tirer au hasard un élément λ non nul de $GF(2^n)$;

2) Calculer $X'1 = \lambda^2 * X1$, $Y'1 = \lambda^3 * Y1$, $Z'1 = \lambda * Z1$,
 $X'1$, $Y'1$ et $Z'1$ définissent les coordonnées

5 du point $P' = (X'1, Y'1, Z'1)$;

3) Calcul de $Q = 2.P'$ à l'aide de l'algorithme A.
Les variables manipulées au cours de l'exécution
du procédé A' étant aléatoire, l'attaque DPA
précédemment décrite ne s'applique plus.

10

Dans ce paragraphe, on décrit la modification de
l'algorithme d'addition de point d'une courbe
elliptique définie sur le corps fini $GF(2^n)$.

15 Les coordonnées projectives du point
 $R = (X2, Y2, Z2)$ tel que $R = P + Q$ avec $P = (X0, Y0, Z0)$ et
 $Q = (X1, Y1, Z1)$ sont calculées par le procédé
suivant en 12 étapes. Dans chacune des étapes,
les calculs sont effectués dans le corps fini

20 $GF(2^n)$.

1) Calculer $U0 = X0 * Z1^2$;

2) Calculer $S0 = Y0 * Z1^3$;

3) Calculer $U1 = X1 * Z0^2$;

4) Calculer $S1 = Y1 * Z0^3$;

25 5) Calculer $W = U0 + U1$;

6) Calculer $R = S0 + S1$;

7) Calculer $L = Z0 * W$;

8) Calculer $V = R * X1 + L * Y1$;

9) Calculer $Z2 = L * Z1$;

30 10) Calculer $T = R + Z2$;

11) Calculer $X2 = a * Z2^2 + T * R + W^3$;

12) Calculer $Y2 = T * X2 + V * L^2$.

Le procédé de la contre mesure consiste en une modification du procédé précédent. Le nouveau procédé d'addition de point d'une courbe elliptique définie sur le corps fini $GF(2^n)$

5 consiste en les 14 étapes suivantes :

- 1) Tirer au hasard un élément λ non nul de $GF(2^n)$;
- 2) Remplacer X_0 par $\lambda^2 \cdot X_0$, Y_0 par $\lambda^3 \cdot Y_0$ et Z_0 par $\lambda \cdot Z_0$;
- 10 3) Tirer au hasard un élément μ non nul de $GF(2^n)$;
- 4) Remplacer X_1 par $\mu^2 \cdot X_1$, Y_1 par $\mu^3 \cdot Y_1$ et Z_1 par $\mu \cdot Z_1$;
- 5) Calculer $U_0 = X_0 \cdot Z_1^2$;
- 15 6) Calculer $S_0 = Y_0 \cdot Z_1^3$;
- 7) Calculer $U_1 = X_1 \cdot Z_0^2$;
- 8) Calculer $S_1 = Y_1 \cdot Z_0^3$;
- 9) Calculer $W = U_0 + U_1$;
- 10) Calculer $R = S_0 + S_1$;
- 20 11) Calculer $L = Z_0 \cdot W$;
- 12) Calculer $V = R \cdot X_1 + L \cdot Y_1$;
- 13) Calculer $Z_2 = L \cdot Z_1$;
- 14) Calculer $T = R + Z_2$;
- 15) Calculer $X_2 = a \cdot Z_2^2 + T \cdot R + W^3$;
- 25 16) Calculer $Y_2 = T \cdot X_2 + V \cdot L^2$;

Plus généralement, le procédé de la contre mesure s'applique quelque soit le procédé (noté par la suite A) utilisé pour réaliser l'opération d'addition de point. Le procédé A

30 est remplacé par le procédé A' en 5 étapes :

Entrée : deux points $P=(X_0, Y_0, Z_0)$ et $Q=(X_1, Y_1, Z_1)$ représentés en coordonnées projectives.

Sortie : le point $R=(X_2, Y_2, Z_2)$ représenté en
5 coordonnées projectives tel que $R=P+Q$

1) Tirer au hasard un élément λ non nul de $GF(2^n)$;

2) Remplacer X_0 par $\lambda^2 \cdot X_0$, Y_0 par $\lambda^3 \cdot Y_0$ et Z_0
10 par $\lambda \cdot Z_0$;

3) Tirer au hasard un élément μ non nul de $GF(2^n)$;

4) Remplacer X_1 par $\mu^2 \cdot X_1$, Y_1 par $\mu^3 \cdot Y_1$ et Z_1
par $\mu \cdot Z_1$;

15 5) Calcul de $R=P+Q$ à l'aide de l'algorithme A.

Les variables manipulées au cours de l'exécution du procédé A' étant aléatoire, l'attaque DPA précédemment décrite ne s'applique plus.

20

Le procédé de la contre mesure consiste également en la définition de 4 variantes dans l'opération de multiplication scalaire.

L'opération de multiplication scalaire fait
25 appel à l'opération de doublement de point noté Do et à l'opération d'addition de point noté Ad .

L'opération de doublement de point modifié décrite précédemment est notée Do' et l'opération d'addition de point modifiée décrite
30 précédemment est notée Ad' .

Dans ce paragraphe on décrit la première variante de modification de l'opération de multiplication scalaire. La première variante consiste à rendre aléatoire la représentation d'un point au début du procédé de calcul. Dans le cas de l'utilisation de l'algorithme "double and add", le procédé modifié de multiplication scalaire est le suivant en 5 étapes. Le procédé prend en entrée un point P et un entier d.

10 L'entier d est noté $d = (d(t), d(t-1), \dots, d(0))$, où $(d(t), d(t-1), \dots, d(0))$ est la représentation binaire de d, avec $d(t)$ le bit de poids fort et $d(0)$ le bit de poids faible. L'algorithme retourne en sortie le point $Q = d.P$.

15 Cette première variante s'exécute en cinq étapes:

- 1) Initialiser le point Q avec la valeur P;
- 2) Remplacer Q par $2.Q$ en utilisant le procédé Do' ;
- 20 3) Si $d(t-1)=1$ remplacer Q par $Q+P$ en utilisant le procédé Ad;
- 4) Pour i allant de $t-2$ à 0 exécuter :
 - 4a) Remplacer Q par $2Q$;
 - 4b) Si $d(i)=1$ remplacer Q par $Q+P$;
- 25 5) Retourner Q.

Plus généralement, le procédé de la première variante décrit précédemment s'applique à l'opération de multiplication scalaire quelque soit le procédé (noté par la suite A) utilisé pour réaliser le calcul de la multiplication scalaire. Le procédé A fait appel aux opérations Do et Ad définies précédemment.

La première variante de la contre mesure consiste à remplacer la première opération Do par Do' définie précédemment.

- 5 La première variante permet donc d'assurer que les variables intermédiaires manipulées lors de l'opération de multiplication scalaire sont aléatoires. Cela rend l'attaque DPA précédemment décrite inapplicable.

10

Dans ce paragraphe on décrit la deuxième variante de modification de l'opération de multiplication scalaire.

- 15 La deuxième variante consiste à rendre aléatoire la représentation d'un point au début du procédé de calcul et à la fin du procédé de calcul. Dans le cas de l'utilisation de l'algorithme " double and add ", le procédé modifié de multiplication scalaire est le suivant en 7 étapes. Le procédé
- 20 prend en entrée un point P et un entier d. L'entier d est noté $d=(d(t), d(t-1), \dots, d(0))$, où $(d(t), d(t-1), \dots, d(0))$ est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. L'algorithme
- 25 retourne en sortie le point $Q=d.P$.

Cette seconde variante s'exécute en sept étapes:

- 1) Initialiser le point Q avec la valeur P;
- 2) Remplacer Q par 2.Q en utilisant le procédé
- 30 Do' ;
- 3) Si $d(t-1)=1$ remplacer Q par $Q+P$ en utilisant le procédé Ad;

- 4) Pour i allant de $t-2$ à 1 exécuter :
- 4a) Remplacer Q par $2Q$;
- 4b) Si $d(i)=1$ remplacer Q par $Q+P$;
- 5) Remplacer Q par $2.Q$ en utilisant le procédé
- 5 Do' ;
- 6) Si $d(0)=1$ remplacer Q par $Q+P$ en utilisant le procédé Ad;
- 7) Retourner Q .

- 10 Plus généralement, le procédé de la deuxième variante décrit précédemment s'applique à l'opération de multiplication scalaire quelque soit le procédé (noté par la suite A) utilisé pour réaliser le calcul de la multiplication
- 15 scalaire. Le procédé A fait appel aux opérations Do et Ad définies précédemment. La deuxième variante de la contre mesure consiste à remplacer la première opération Do par Do' définie précédemment et la dernière opération Do
- 20 par Do'.

La deuxième variante permet donc d'assurer que les variables intermédiaires manipulées lors de l'opération de multiplication scalaire sont

25 aléatoires. L'avantage de la deuxième variante est une sécurité accrue contre des attaques DPA en fin d'algorithme de multiplication scalaire. En particulier, la deuxième variante rend l'attaque DPA précédemment décrite inapplicable.

30

Dans ce paragraphe, on décrit la troisième variante de modification de l'opération de multiplication scalaire.

La troisième variante consiste à rendre aléatoire la représentation de chacun des points manipulés au cours du procédé de multiplication scalaire. Dans le cas de l'utilisation de l'algorithme "double and add", le procédé modifié de multiplication scalaire est le suivant en 4 étapes. Le procédé prend en entrée un point P et un entier d. L'entier d est noté $d=(d(t), d(t-1), \dots, d(0))$, où $(d(t), d(t-1), \dots, d(0))$ est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. L'algorithme retourne en sortie le point $Q=d.P$.

Cette troisième variante s'exécute en trois étapes:

- 1) Initialiser le point Q avec le point P;
- 2) Pour i allant de t-2 à 0 exécuter :
 - 2a) Remplacer Q par 2Q en utilisant le procédé Do';
 - 2b) Si $d(i)=1$ remplacer Q par $Q+P$ en utilisant le procédé Ad';
- 3) Retourner Q.

25

Plus généralement, le procédé de la troisième variante décrit précédemment s'applique à l'opération de multiplication scalaire quelque soit le procédé (noté par la suite A) utilisé pour réaliser le calcul de la multiplication scalaire. Le procédé A fait appel aux opérations Do et Ad définies précédemment.

30

La troisième variante de la contre mesure consiste à remplacer toutes les opérations Do par Do' et Ad par Ad'.

5 La troisième variante permet donc d'assurer que les variables intermédiaires manipulées lors de l'opération de multiplication scalaire sont aléatoires. L'avantage de la troisième variante par rapport à la deuxième variante est une
10 sécurité accrue contre les attaques DPA sur les opérations intermédiaires du procédé de multiplication scalaire. En particulier, la troisième variante rend l'attaque DPA précédemment décrite inapplicable.

15

Dans ce paragraphe on décrit la quatrième variante de modification de l'opération de multiplication scalaire. La quatrième variante consiste à rendre aléatoire la représentation de
20 chacun des points manipulés au cours du procédé de multiplication scalaire. La quatrième variante est une modification de la troisième variante par l'utilisation d'un compteur, ledit compteur permettant de déterminer les étapes de
25 l'algorithme de multiplication scalaire pour lesquelles la représentation d'un point est rendue aléatoire. On définit pour cela un paramètre de sécurité T. Dans la pratique on peut prendre $T=5$. Dans le cas de l'utilisation
30 de l'algorithme "double and add", le procédé modifié de multiplication scalaire est le suivant en 4 étapes. Le procédé prend en entrée un point P et un entier d.

L'entier d est noté $d=(d(t),d(t-1),\dots, d(0))$, où $(d(t),d(t-1),\dots,d(0))$ est la représentation binaire de d , avec $d(t)$ le bit de poids fort et $d(0)$ le bit de poids faible. L'algorithme
5 retourne en sortie le point $Q=d.P$.

La quatrième variante s'exécute en trois étapes:

- 1) Initialiser le point Q avec le point P
- 10 2) Initialiser le compteur co à la valeur T .
- 3) Pour i allant de $t-1$ à 0 exécuter :
 - 3a) Remplacer Q par $2Q$ en utilisant le procédé Do si co est différent de 0 , sinon utiliser le procédé Do' .
 - 15 3b) Si $d(i)=1$ remplacer Q par $Q+P$ en utilisant le procédé Ad .
 - 3c) Si $co=0$ alors réinitialiser le compteur co à la valeur T .
 - 3d) Décrémenter le compteur co .
- 20 3) Retourner Q .

Plus généralement, le procédé de la troisième variante décrit précédemment s'applique à l'opération de multiplication scalaire quelque
25 soit le procédé (noté par la suite A) utilisé pour réaliser le calcul de la multiplication scalaire. Le procédé A fait appel aux opérations Do et Ad définies précédemment.

La variante de la troisième contre mesure
30 consiste à initialiser un compteur co à la valeur T . L'opération Do est remplacée par l'opération Do' si la valeur du compteur est égale à 0 .

Après chaque exécution des opérations Do ou Do', le compteur est réinitialisé à la valeur T s'il a atteint la valeur 0 ; il est ensuite décrémenté.

5

La quatrième variante permet donc d'assurer que les variables intermédiaires manipulées lors de l'opération de multiplication scalaire sont aléatoires. L'avantage de la quatrième variante par rapport à la troisième variante est une plus grande rapidité d'exécution. La quatrième variante rend l'attaque DPA précédemment décrite inapplicable.

10

15 L'application de l'une des 4 variantes précédemment décrite permet donc de protéger tout algorithme cryptographique basé sur les courbes elliptiques contre l'attaque de type DPA précédemment décrite.

20

REVENDICATIONS

1- Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé publique de type courbe elliptique en utilisant la représentation des points de ladite courbe elliptique en coordonnées projectives consistant à représenter un point P de la courbe elliptique par les coordonnées (X, Y, Z) telles que $x=X/Z$ et $y=Y/Z^3$, x et y étant les coordonnées du point de la courbe elliptique en coordonnées affines, ladite courbe comprenant n éléments et étant définie sur un corps fini $GF(p)$, p étant un nombre premier, ladite courbe ayant pour équation $y^2=x^3+a*x+b$, ou définie sur un corps fini $GF(2^n)$, ladite courbe ayant pour équation $y^2+x*y=x^3+a*x^2+b$, où a et b sont des paramètres entiers fixés au départ, ledit procédé étant caractérisé en ce qu'il choisit un représentant aléatoire parmi n éléments possibles en coordonnées projectives de la courbe elliptique et consiste en une modification des opérations d'addition de points et le doublement desdits points et une modification de l'opération de multiplication scalaire.

2- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que le procédé de la contre mesure s'applique quelque soit le procédé ou algorithme, noté par la suite A, utilisé pour réaliser l'opération de doublement de point, le procédé A étant remplacé par le procédé A' en 3 étapes, en utilisant une entrée définie par un point $P=(X1,Y1,Z1)$ représenté en coordonnées projectives et une sortie définie par un point $Q=(X2,Y2,Z2)$ représenté en coordonnées projectives tel que $Q=2.P$, de la courbe elliptique, lesdites étapes étant:

- 15 1) Tirer au hasard un entier λ tel que $0 < \lambda < p$;
- 2) Calculer $X'1 = \lambda^2 * X1$, $Y'1 = \lambda^3 * Y1$ et $Z'1 = \lambda * Z1$; $X'1$, $Y'1$ et $Z'1$ définissant les coordonnées du point $P'=(X'1,Y'1,Z'1)$;
- 3) Calculer $Q=2*P'$ à l'aide de l'algorithme A.

20

3- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que l'algorithme de doublement de points, ou opérations de doublement de points d'une courbe elliptique défini sur ledit corps fini $GF(p)$ s'effectue en huit étapes:

- 1) Tirer au hasard un entier λ tel que $0 < \lambda < p$;
- 2) Calculer $X'1 = \lambda^2 * X1$, $Y'1 = \lambda^3 * Y1$ et $Z'1 = \lambda * Z1$;
- 30 3) Calculer $M = 3 * X'1^2 + a * Z'1^4$;
- 4) Calculer $Z2 = 2 * Y'1 * Z'1$;
- 5) Calculer $S = 4 * X'1 * Y'1^2$;
- 6) Calculer $X2 = M^2 - 2 * S$;
- 7) Calculer $T = 8 * Y'1^4$;
- 35 8) Calculer $Y2 = M * (S - X2) - T$.

- 4- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que plus généralement le procédé de la contre-mesure s'applique quelque soit le procédé noté par la suite A utilisé pour réaliser l'opération d'addition de points sur une courbe elliptique défini sur ledit corps fini $GF(p)$ s'effectue en cinq étapes :
- 10 1) Tirer au hasard un élément λ non nul de $GF(2^n)$;
 - 2) Remplacer X_0 par $\lambda^2 \cdot X_0$, Y_0 par $\lambda^3 \cdot Y_0$ et Z_0 par $\lambda \cdot Z_0$;
 - 3) Tirer au hasard un élément μ non nul de $GF(2^n)$;
 - 15 4) Remplacer X_1 par $\mu^2 \cdot X_1$, Y_1 par $\mu^3 \cdot Y_1$ et Z_1 par $\mu \cdot Z_1$;
 - 5) Calcul de $R=P+Q$ à l'aide de l'algorithme A.
- 20 5- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la modification de l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini $GF(p)$, où p est un nombre premier, est la suivante: les coordonnées projectives du point $R=(X_2, Y_2, Z_2)$ tel que $R=P+Q$ avec $P=(X_0, Y_0, Z_0)$ et $Q=(X_1, Y_1, Z_1)$ sont calculées par le procédé suivant en 16 étapes, dans chacune des étapes, les calculs étant effectués modulo p :
- 30
- 1) Tirer au hasard un entier λ appartenant audit corp fini $GF(p)$ tel que $0 < \lambda < p$;
 - 2) Remplacer X_0 par $\lambda^2 \cdot X_0$, Y_0 par $\lambda^3 \cdot Y_0$ et Z_0 par $\lambda \cdot Z_0$;

- 3) Tirer au hasard un entier μ appartenant à tel que $0 < \mu < p$;
- 4) Remplacer X_1 par $\mu^2 \cdot X_1$, Y_1 par $\mu^3 \cdot Y_1$ et Z_1 par $\mu \cdot Z_1$;
- 5) 5) Calculer $U_0 = X_0 \cdot Z_1^2$;
- 6) 6) Calculer $S_0 = Y_0 \cdot Z_1^3$;
- 7) 7) Calculer $U_1 = X_1 \cdot Z_0^2$;
- 8) 8) Calculer $S_1 = Y_1 \cdot Z_0^3$;
- 9) 9) Calculer $W = U_0 - U_1$;
- 10) 10) Calculer $R = S_0 - S_1$;
- 11) 11) Calculer $T = U_0 + U_1$;
- 12) 12) Calculer $M = S_0 + S_1$;
- 13) 13) Calculer $Z_2 = Z_0 \cdot Z_1 \cdot W$;
- 14) 14) Calculer $X_2 = R^2 - T \cdot W^2$;
- 15) 15) Calculer $V = T \cdot W^2 - 2 \cdot X_2$;
- 16) 16) Calculer $2 \cdot Y_2 = V \cdot R - M \cdot W^3$.
- 6- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que plus généralement, la modification de l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini $GF(2^n)$, où n est un nombre premier, est la suivante: les coordonnées projectives du point $P = (X_1, Y_1, Z_1)$ tel que $R = P + Q$ et $Q = (X_2, Y_2, Z_2)$ sont calculées par le procédé suivant en 3 étapes, dans chacune des étapes, les calculs étant effectués modulo p :
- 1) Tirer au hasard un élément λ non nul de $GF(2^n)$;
- 2) Calculer $X'_1 = \lambda^2 \cdot X_1$, $Y'_1 = \lambda^3 \cdot Y_1$, $Z'_1 = \lambda \cdot Z_1$,
- 30 X'_1 , Y'_1 et Z'_1 définissent les coordonnées du point $P' = (X'_1, Y'_1, Z'_1)$;
- 3) Calcul de $Q = 2 \cdot P'$ à l'aide de l'algorithme A.

7- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que le procédé de la contre mesure consiste en une modification du procédé précédent, le nouveau procédé de
5 doublement de point d'une courbe elliptique étant définie sur le corps fini $GF(2^n)$, et consiste en les 6 étapes suivantes :

- 1) Tirer au hasard un élément non nul λ de
10 $GF(2^n)$;
- 2) Calculer $X'1 = \lambda^2 * X1$, $Y'1 = \lambda^3 * Y1$, $Z'1 = \lambda * Z1$;
- 3) Calculer $Z2 = X'1 * Z'1^2$;
- 4) Calculer $X2 = (X'1 + c * Z'1^2)^4$;
- 5) Calculer $U = Z2 + X'1^2 + Y'1 * Z'1$;
- 15 6) Calculer $Y2 = X'1^4 * Z2 + U * X2$.

8 - Procédé de contre-mesure selon la revendication 1 caractérisé en ce que
Plus généralement, la modification de
20 l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini $GF(2^n)$, où n est un nombre premier, est la suivante: les coordonnées projectives du point $P = (X0, Y0, Z0)$ et $Q = (X1, Y1, Z2)$ en entrée et $R = (X2, Y2, Z2)$ sont
25 calculées par le procédé suivant en 5 étapes, dans chacune des étapes, les calculs étant effectués modulo:

- 1) Tirer au hasard un élément λ non nul de
30 $GF(2^n)$;
- 2) Remplacer $X0$ par $\lambda^2 * X0$, $Y0$ par $\lambda^3 * Y0$ et $Z0$ par $\lambda * Z0$;
- 3) Tirer au hasard un élément μ non nul de $GF(2^n)$;

4) Remplacer X_1 par $\mu^2 \cdot X_1$, Y_1 par $\mu^3 \cdot Y_1$ et Z_1 par $\mu \cdot Z_1$;

5) Calcul de $R=P+Q$ à l'aide de l'algorithme A.

5 9- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que le procédé de la contre mesure consiste en une modification du procédé d'addition de points d'une courbe elliptique définie sur le corps fini $GF(2^n)$ et
10 consiste en les 16 étapes suivantes :

1) Tirer au hasard un élément λ non nul de $GF(2^n)$;

2) Remplacer X_0 par $\lambda^2 \cdot X_0$, Y_0 par $\lambda^3 \cdot Y_0$ et Z_0 par $\lambda \cdot Z_0$;

3) Tirer au hasard un élément μ non nul de $GF(2^n)$;

4) Remplacer X_1 par $\mu^2 \cdot X_1$, Y_1 par $\mu^3 \cdot Y_1$ et Z_1 par $\mu \cdot Z_1$;

20 5) Calculer $U_0 = X_0 \cdot Z_1^2$;

6) Calculer $S_0 = Y_0 \cdot Z_1^3$;

7) Calculer $U_1 = X_1 \cdot Z_0^2$;

8) Calculer $S_1 = Y_1 \cdot Z_0^3$;

9) Calculer $W = U_0 + U_1$;

25 10) Calculer $R = S_0 + S_1$;

11) Calculer $L = Z_0 \cdot W$;

12) Calculer $V = R \cdot X_1 + L \cdot Y_1$;

13) Calculer $Z_2 = L \cdot Z_1$;

14) Calculer $T = R + Z_2$;

30 15) Calculer $X_2 = a \cdot Z_2^2 + T \cdot R + W^3$;

16) Calculer $Y_2 = T \cdot X_2 + V \cdot L^2$;

10 - Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la première variante de modification de l'opération de multiplication scalaire consiste à rendre aléatoire la représentation d'un point au début du procédé de calcul par l'utilisation de l'algorithme "double and add", le procédé modifié, de multiplication scalaire est le suivant en 5 étapes, en prenant en entrée un point P et un entier d, l'entier d étant noté $d=(d(t), d(t-1), \dots, d(0))$, où $(d(t), d(t-1), \dots, d(0))$ est la représentation binaire de d, avec $d(t)$ le bit de poids fort et $d(0)$ le bit de poids faible, l'algorithme retournant en sortie le point $Q=d.P$, le procédé Do étant le procédé de doublement de points, le procédé Do' étant le procédé de doublement des points modifiés suivant l'une quelconque des revendications précédentes, cette première variante s'exécutant en cinq étapes:

- 1) Initialiser le point Q avec la valeur P;
- 2) Remplacer Q par $2.Q$ en utilisant le procédé Do';
- 3) Si $d(t-1)=1$ remplacer Q par $Q+P$ en utilisant le procédé Ad, le procédé Ad étant le procédé d'addition de points;
- 4) Pour i allant de $t-2$ à 0 exécuter :
 - 4a) Remplacer Q par $2Q$;
 - 4b) Si $d(i)=1$ remplacer Q par $Q+P$;
- 5) Retourner Q.

11- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la deuxième variante de l'opération de multiplication scalaire consiste à rendre aléatoire la représentation d'un point au début du procédé de calcul et à la fin du procédé de calcul, ceci dans le cas de l'utilisation de l'algorithme "double and add",

le procédé modifié de multiplication scalaire étant le suivant en 7 étapes, prenant en entrée un point P et un entier d, l'entier d étant noté $d=(d(t), d(t-1), \dots, d(0))$, où $(d(t), d(t-1), \dots, d(0))$ est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible, l'algorithme retournant en sortie le point $Q=d.P$, ladite seconde variante s'exécutant en sept étapes:

- 1) Initialiser le point Q avec la valeur P;
- 2) Remplacer Q par 2.Q en utilisant le procédé Do' ;
- 3) Si $d(t-1)=1$ remplacer Q par $Q+P$ en utilisant le procédé Ad;
- 4) Pour i allant de t-2 à 1 exécuter :
 - 4a) Remplacer Q par 2Q;
 - 4b) Si $d(i)=1$ remplacer Q par $Q+P$;
- 5) Remplacer Q par 2.Q en utilisant le procédé Do' ;
- 6) Si $d(0)=1$ remplacer Q par $Q+P$ en utilisant le procédé Ad;
- 7) Retourner Q.

12- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la troisième variante de l'opération de multiplication scalaire s'exécute en trois étapes:

- 1) Initialiser le point Q avec le point P;
- 2) Pour i allant de t-2 à 0 exécuter :
 - 2a) Remplacer Q par 2Q en utilisant le
5 procédé Do';
 - 2b) Si $d(i)=1$ remplacer Q par Q+P en
utilisant le procédé Ad', Ad' étant le procédé
d'addition des points modifiés suivant les
revendications précédentes;
- 10 3) Retourner Q.

13- Procédé de contre-mesure selon la
revendication 1 caractérisé en ce que la
quatrième variante de l'opération de
15 multiplication scalaire s'exécute en trois
étapes:

- 1) Initialiser le point Q avec le point P
- 2) Initialiser le compteur co à la valeur T.
- 3) Pour i allant de t-1 à 0 exécuter :
 - 20 3a) Remplacer Q par 2Q en utilisant le
procédé Do si co est différent de 0, sinon
utiliser le procédé Do'.
 - 3b) Si $d(i)=1$ remplacer Q par Q+P en
utilisant le procédé Ad.
 - 25 3c) Si co=0 alors réinitialiser le compteur co
à la valeur T.
 - 3d) Décrémenter le compteur co.
- 3) Retourner Q.

14- Composant électronique utilisant le procédé
30 selon l'une quelconque des revendications
précédentes caractérisé en ce qu'il peut être
une carte à puce.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 00/00603

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MENEZES A J ET AL: "ELLIPTIC CURVE CRYPTOSYSTEMS AND THEIR IMPLEMENTATION" JOURNAL OF CRYPTOLOGY, US, NEW YORK, NY, vol. 6, no. 4, September 1993 (1993-09), pages 209-224, XP002069135 abstract page 209, last paragraph -page 210, paragraph 1 page 216, line 17 -page 217, line 15	1

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"Z" document member of the same patent family

Date of the actual completion of the international search

31 May 2000

Date of mailing of the international search report

09/06/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Des le Internationale No

PCT/FR 00/00603

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/30 G06F7/72

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	MENEZES A J ET AL: "ELLIPTIC CURVE CRYPTOSYSTEMS AND THEIR IMPLEMENTATION" JOURNAL OF CRYPTOLOGY, US, NEW YORK, NY, vol. 6, no. 4, septembre 1993 (1993-09), pages 209-224, XP002069135 abrégé page 209, dernier alinéa -page 210, alinéa 1 page 216, ligne 17 -page 217, ligne 15	1

☐ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

A document définissant l'état général de la technique, non considéré comme particulièrement pertinent

E document antérieur, mais publié à la date de dépôt international ou après cette date

L document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

O document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

P document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

T document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

X document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

Y document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

Z document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

31 mai 2000

Date d'expédition du présent rapport de recherche internationale

09/06/2000

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040. Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Holper, G